Prudential Practice Guide

CPG 230 Operational Risk Management

June 2024

AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY | APRA.GOV.AU

Contents

About this guide....2
Glossary....3
Key principles....4
Risk management framework....5
Roles and responsibilities....7
Operational risk management....9
Business continuity....13
Management of service provider arrangements....17

About this guide

Prudential practice guides (PPGs) share APRA's views on sound practice. They discuss requirements from legislation, regulations or APRA's prudential standards, but do not themselves create enforceable requirements.

This PPG offers guidance to APRA-regulated entities to aid compliance with *Prudential Standard CPS 230 Operational Risk Management* (CPS 230). CPS 230 sits within the Risk Management pillar of APRA's framework, as a supporting standard.

Effective operational risk management is essential to ensure the resilience of an entity, and its ability to maintain critical operations through disruptions.

Proportionality

CPS 230 applies to every APRA-regulated entity. Each one, regardless of size, has operational risks which can crystalise and adversely affect their depositors, policyholders or beneficiaries.

CPS 230 sets baseline expectations for all entities. APRA expects significant financial institutions (SFIs) to have stronger practices, commensurate with the size and complexity of their operations. All entities should mature their practice over time, as business operations grow and evolve, and to match the scale of their risks and role in the financial system.

Reading this guide

> Relevant paragraphs from CPS 230 (enforceable requirements) are in blue boxes. The remainder of the text is guidance. Footnotes in CPS 230 have not been reproduced in this document.

Glossary

Accountable person	Accountable person as defined in sections 10 and 11 of the *Financial Accountability Regime Act 2023*
ADI	Authorised deposit-taking institution, as defined in the *Banking Act 1959*
APRA	Australian Prudential Regulation Authority
APS 001	*Prudential Standard APS 001 Definitions*
ASIC	Australian Securities and Investments Commission
BCP	Business continuity plan
Board	Board of directors
CPS 220	*Prudential Standard CPS 220 Risk Management*
CPS 230	*Prudential Standard CPS 230 Operational Risk Management*
CPS 234	*Prudential Standard CPS 234 Information Security*
Critical operations	Processes undertaken by an APRA-regulated entity or its service provider which, if disrupted beyond tolerance levels, would have a material adverse impact on its depositors, policyholders, beneficiaries or other customers, or its role in the financial system
GPS 001	*Prudential Standard GPS 001 Definitions*
HPS 001	*Prudential Standard HPS 001 Definitions*
LPS 001	*Prudential Standard LPS 001 Definitions*
Material arrangements	Material arrangements are those on which an APRA-regulated entity relies to undertake a critical operation or that expose it to material operational risk
Material service providers	Material service providers are those on which an APRA-regulated entity relies to undertake a critical operation or that expose it to material operational risk
RSE	Registrable Superannuation Entity
RSE licensee	RSE licensee as defined in subsection 10(1) of the SIS Act
SIS Act	*Superannuation Industry (Supervision) Act 1993*
SPS 220	*Prudential Standard SPS 220 Risk Management*

Key principles

12. An APRA-regulated entity must:

(a) effectively manage its operational risks, and set and maintain appropriate standards for conduct and compliance;

(b) maintain its critical operations within tolerance levels through severe disruptions; and

(c) manage the risks associated with the use of service providers.

13. An APRA-regulated entity must identify, assess and manage operational risks that may result from inadequate or failed internal processes or systems, the actions or inactions of people or external drivers and events. Operational risk is inherent in all products, activities, processes and systems.

14. An APRA-regulated entity must, to the extent practicable, prevent disruption to critical operations, adapt processes and systems to continue to operate within tolerance levels in the event of a disruption and return to normal operations promptly once a disruption is over.

15. An APRA-regulated entity must not rely on a service provider unless it can ensure that in doing so it can continue to meet its prudential obligations in full and effectively manage the associated risks.

1. The aim of CPS 230 is to ensure that APRA-regulated entities ('entities') are resilient to operational risks and disruptions. Operational resilience is the outcome of prudent operational risk management: the ability to effectively manage and control operational risks; limit disruptions; and maintain critical operations through disruptions.

2. APRA expects that, in implementing CPS 230, a prudent entity would start with the identification of its critical operations. An entity would:

    a) identify its critical operations (paragraph 36 of CPS 230 sets out the minimum list);

    b) set tolerance levels for disruption of these critical operations; and

    c) identify the processes and resources needed to deliver these critical operations, including material service providers.

3. A prudent entity would then use this information as the starting point for an assessment of its operational risk profile.

Risk management framework

16. As part of its risk management framework required under *Prudential Standard CPS 220 Risk Management* (CPS 220) and *Prudential Standard SPS 220 Risk Management* (SPS 220), an APRA-regulated entity must develop and maintain:

(a) governance arrangements for the oversight of operational risk;

(b) an assessment of its operational risk profile, with a defined risk appetite supported by indicators, limits and tolerance levels;

(c) internal controls that are designed and operating effectively for the management of operational risks;

(d) appropriate monitoring, analysis and reporting of operational risks and escalation processes for operational incidents and events;

(e) business continuity plan(s) (BCPs) that set out how the entity would identify, manage and respond to a disruption within tolerance levels and are regularly tested with severe but plausible scenarios; and

(f) processes for the management of service provider arrangements.

17. As part of the required reviews of the risk management framework under CPS 220 and SPS 220, an APRA-regulated entity must review its operational risk management. The reviews must cover those aspects of operational risk management set out in paragraph 16.

18. Operational risk management must be integrated into an APRA-regulated entity's overall risk management framework and processes. Business continuity planning must be consistent with, and not conflict or undermine, an APRA-regulated entity's recovery and exit planning.

19. Where APRA considers that an APRA-regulated entity's operational risk management has material weaknesses, APRA may:

(a) require an independent review of the entity's operational risk management;

(b) require the entity to develop a remediation program;

(c) require the entity to hold additional capital, as relevant;

(d) impose conditions on the entity's licence; and

(e) take other actions required in the supervision of this Prudential Standard.

4. CPS 230 builds on the general risk management requirements in *Prudential Standard CPS 220 Risk Management* (CPS 220) and *Prudential Standard SPS 220 Risk Management* (SPS 220), with more specific requirements for the management of operational risks.

5. Where an entity has identified material weaknesses in its operational risk management, APRA expects that the entity would keep APRA informed of the progress of the entity's remediation.

6. APRA's prudential standards for ADIs and insurers require that operational risk capital reflects the operational risk profile of the entity.[1] Generally, where there are material weaknesses in the management of operational risk, APRA expects an ADI or insurer would hold additional capital until remediation is complete. This may be through an overlay determined by senior management, required by the Board or applied by APRA.

[1] APRA requires ADIs and insurers to hold capital for operational risks, as prescribed *by Prudential Standard APS 115 Capital Adequacy: Standardised Measurement Approach to Operational Risk* (APS 115), *Prudential Standard GPS 118 Capital Adequacy: Operational Risk Charge* (GPS 118), *Prudential Standard LPS 118 Capital Adequacy: Operational Risk Charge* (LPS 118) and *Prudential Standard HPS 118 Capital Adequacy: Operational Risk Charge* (HPS 118).

Roles and responsibilities

20. The Board of an APRA-regulated entity is ultimately accountable for oversight of an entity's operational risk management. This includes business continuity and the management of service provider arrangements.

21. The Board must ensure that the APRA-regulated entity sets clear roles and responsibilities for senior managers for operational risk management, including business continuity and the management of service provider arrangements.

22. The Board must:

(a) oversee operational risk management and the effectiveness of key internal controls in maintaining the entity's operational risk profile within risk appetite. The Board must be provided with regular updates on the APRA-regulated entity's operational risk profile and ensure senior management takes action as required to address any areas of concern;

(b) approve the BCP and tolerance levels for disruptions to critical operations, review the results of testing and oversee the execution of any findings; and

(c) approve the service provider management policy, and review risk and performance reporting on material service providers.

23. Senior management of an APRA-regulated entity must provide clear and comprehensive information to the Board on the expected impacts on the entity's critical operations when the Board is making decisions that could affect the resilience of critical operations.

The Board

Allocate responsibility

7. A prudent Board would have a clear understanding of who is responsible within the entity for each aspect of operational risk management, including business continuity and the management of service provider arrangements. It should have reasonable assurance that there are no gaps in responsibilities.

8. Processes for delegation from, and reporting to, the Board and senior management should be clear and documented, including for the escalation of risks and issues.

Oversee the risk profile

9. The Board would typically:

   a) oversee updates to an entity's operational risk profile and ensure risks outside of its appetite are addressed promptly;

   b) oversee the effectiveness of key internal controls;

c) be kept informed of areas of any material weaknesses and major remediation efforts;

d) understand the material operational risks that arise from new ventures; and

e) ensure internal audit provides assurance and has appropriate capabilities for this task.

Challenge and approve

10. The Board, in approving the BCP and overall tolerances for the disruption of critical operations, would also ensure that the BCP aligns with its tolerances.

11. While the Board approves the service provider management policy, it may delegate approval of non-material changes.

Senior management

12. Senior managers play an important role in equipping Boards to make effective decisions. APRA expects that information provided to the Board is targeted and timely.

13. Boards may delegate to senior management the ability to approve more granular policies, tolerance levels and plans which sit beneath, and align to, Board-approved documents.

Notifying APRA

14. Where CPS 230 requires notification to APRA (see Table 1), it is to be made electronically using the form on APRA's web site.

Table 1. Notifications to APRA

Notifications to APRA[2]	
Operational risk incidents	As soon as possible and not later than 72 hours after becoming aware of an operational risk incident that it determines to be likely to have a material financial impact or a material impact on the ability of the entity to maintain its critical operations (paragraph 33 of CPS 230)
Disruption	As soon as possible and not later than 24 hours after a disruption to a critical operation outside of tolerance (paragraph 42 of CPS 230)
Material services	As soon as possible and not later than 20 business days after entering into or materially changing an agreement (paragraph 59(a) of CPS 230)
Offshoring	Before entering into, or when there is a significant change to an offshoring agreement with a material service provider (paragraph 59(b) of CPS 230)

[2] Notification to APRA of an information security incident under CPS 234 does not need to be separately reported under CPS 230. Where a notification falls into two different notification categories, the requirement for notification to APRA is the shorter notification timeframe.

Operational risk management

24. An APRA-regulated entity must manage its full range of operational risks, including but not limited to legal risk, regulatory risk, compliance risk, conduct risk, technology risk, data risk and change management risk. Senior management are responsible for operational risk management across the end-to-end process for all business operations.

25. An APRA-regulated entity must maintain appropriate and sound information and information technology (IT) capability to meet its current and projected business requirements and to support its critical operations and risk management. In managing technology risks, an APRA-regulated entity must monitor the age and health of its information assets and meet the requirements for information security in *Prudential Standard CPS 234 Information Security* (CPS 234).

Operational risk profile and assessment

26. An APRA-regulated entity must assess the impact of its business and strategic decisions on its operational risk profile and operational resilience, as part of its business and strategic planning processes. This must include an assessment of the impact of new products, services, geographies and technologies on its operational risk profile.

27. An APRA-regulated entity must maintain a comprehensive assessment of its operational risk profile. As part of this, an APRA-regulated entity must:

(a) maintain appropriate and effective information systems to monitor operational risk, compile and analyse operational risk data and facilitate reporting to the Board and senior management;

(b) identify and document the processes and resources needed to deliver critical operations, including people, technology, information, facilities and service providers, the interdependencies across them, and the associated risks, obligations, key data and controls; and

(c) undertake scenario analysis to identify and assess the potential impact of severe operational risk events, test its operational resilience and identify the need for new or amended controls and other mitigation strategies.

28. An APRA-regulated entity must conduct a comprehensive risk assessment before providing a material service to another party, to ensure that the APRA-regulated entity is able to continue to meet its prudential obligations after entering into the arrangement. APRA may require an APRA-regulated entity to review and strengthen internal controls or processes where APRA considers there to be heightened prudential risks in such circumstances.

Operational risk controls

29. An APRA-regulated entity must design, implement and embed internal controls to mitigate its operational risks in line with its risk appetite and meet its compliance obligations.

30. An APRA-regulated entity must regularly monitor, review and test controls for design and operating effectiveness, the frequency of which must be commensurate with the materiality of the risks being controlled.

The results of testing must be reported to senior management and any gaps or deficiencies in the control environment must be rectified in a timely manner.

31. An APRA-regulated entity must remediate material weaknesses in its operational risk management, including control gaps, weaknesses and failures. This remediation must be supported by clear accountabilities and assurance and address the root causes of weaknesses in a timely manner. An APRA-regulated entity must include identified control gaps, weaknesses, and failures in its operational risk profile until such matters are remediated.

Operational risk incidents

32. An APRA-regulated entity must ensure that operational risk incidents and near misses are identified, escalated, recorded and addressed in a timely manner. An APRA-regulated entity must take incidents and near misses into account in its assessment of its operational risk profile and control effectiveness in a timely manner.

33. An APRA-regulated entity must notify APRA as soon as possible, and not later than 72 hours, after becoming aware of an operational risk incident that it determines to be likely to have a material financial impact or a material impact on the ability of the entity to maintain its critical operations.

Identify critical operations

15. APRA expects that, in identifying its critical operations, an entity would focus on outward-facing services to support depositors, policyholders, beneficiaries and other customers, as well as the broader financial system and its role therein.

16. In identifying critical operations, in addition to APRA's minimum list (see CPS 230 paragraph 36), a prudent entity would consider business operations that, if disrupted beyond tolerance levels:

    a) would have a direct material adverse impact on depositors, policyholders, beneficiaries or other customers;

    b) would have an indirect material adverse impact on depositors, policyholders, beneficiaries or other customers, such as through significantly impacting the entity's profitability, financial soundness, reputation or ability to comply with legal or regulatory requirements; or

    c) could impact the broader financial system or economy, including through flow-on effects or contagion.

17. APRA expects that 'critical functions' as determined by APRA under *Prudential Standard CPS 900 Resolution Planning* (CPS 900) would also be classified as critical operations.

18. APRA expects that where an entity determines that a business operation prescribed by APRA is not a critical operation, the reasons would be documented, approved by an Accountable person, and reviewed on at least an annual basis. It is not necessary to provide the documented reasoning to APRA, unless APRA specifically asks an entity to provide this information.

Identify processes and resources needed to deliver critical operations

19. Senior management should be satisfied that they have sufficient detail about the resources and processes needed to deliver critical operations. It is important to understand how critical operations are delivered during business-as-usual and maintained in a disruption.

20. Prudent entities will incorporate documented processes into their broader operational risk management framework and ensure it is kept up to date. The more comprehensive the information, the better equipped entities will be to make decisions and take appropriate action.

Maintain an operational risk profile

21. A prudent entity would regularly update their risk profile to reflect changes in strategy, risk environment or business mix.

22. Risk profiles should also be informed by scenario analysis which test severe but plausible events. Scenario analysis helps entities to identify gaps or opportunities to improve their management of operational risk.

Table 2. Steps to assess operational risk profile

Operational risk profile	
Context	Consider the business environment and changes within the business.
Critical Operations	Identify the business' critical operations, and the processes and resources required to provide them.
Risks	Identify and record operational risks within the business, including causes and inherent and residual (post-control) ratings.
Controls	Identify and record controls used to mitigate risks. Assess the efficacy of controls. Test results and any gaps and weaknesses.
Risk appetite	Assess performance against risk appetite.
Actions	Develop and document actions or remediation plans for higher-rated risks or those exceeding appetite. Accept risks where appropriate.

Maintain effective controls (design, test, monitor)

23. Entities should design, implement and embed effective internal controls. To the extent possible, controls should minimise the likelihood and impact of disruptions – particularly to critical operations. Testing would be conducted by staff and teams independent of those with operational responsibility for controls.

24. To monitor, review and test the effectiveness of controls, entities could consider:

    a) the use of consistent criteria across the entity;

    b) design and operating effectiveness;

c) testing of controls for material risks more frequently than for less material risks;

d) capturing of all controls, including those owned by related parties and service providers;

e) having a mix of preventative, detective and corrective controls;

f) having a mix of automated and manual controls;

g) if recent issues and incidents are within appetite or controls need to be adjusted;

h) recording the rationale for the control effectiveness assessment; and

i) any recent changes in the environment or business strategies that could impact control effectiveness.

25. APRA expects that any gaps, weaknesses or failures in controls are identified, escalated and rectified in a timely manner.

Manage and record incidents, remediate

26. Entities would typically have mechanisms to manage all stages of an incident, whether occurring sequentially or concurrently.

Table 3. Steps in managing incidents

Managing incidents	
Detect	Detect incident using automated controls and/or manual review.
Escalate	Escalate so that decision-makers are aware of the incident and to trigger response.
Contain	Contain to minimise damage.
Respond	Respond and remediate.
Review	Analyse and review after the incident, to improve incident management procedures, and support attribution and restitution (where relevant).

27. A prudent entity would identify the root cause of an incident and take steps to remediate. This lessens the chance of the incident recurring and helps to identify any common underlying weaknesses in other products, business areas, the control framework or risk culture.

28. Effective management responses to control weaknesses often include tactical responses (temporary controls or monitoring), followed by strategic solutions (changes to processes, people or systems) to mitigate the risk over the long term.

29. APRA expects that an entity would avoid extended delays or unwarranted extensions to targeted closure dates in addressing operational risk incidents. Incidents and near misses would be recorded in the entity's operational risk information system and linked to controls to ensure that the risk profile accurately reflects any control weaknesses or gaps.

Business continuity

34. An APRA-regulated entity must:

(a) define, identify and maintain a register of its critical operations;

(b) take reasonable steps to minimise the likelihood and impact of disruptions to its critical operations;

(c) maintain a credible BCP that sets out how it would maintain its critical operations within tolerance levels through disruptions, including disaster recovery planning for critical information assets;

(d) activate its BCP if needed in the event of a disruption; and

(e) return to normal operations promptly after a disruption is over.

Critical operations and tolerance levels

35. Critical operations are processes undertaken by an APRA-regulated entity or its service provider which, if disrupted beyond tolerance levels, would have a material adverse impact on its depositors, policyholders, beneficiaries or other customers, or its role in the financial system.

36. An APRA-regulated entity must, at a minimum, classify the following business operations as critical operations, unless it can justify otherwise:

(a) for an ADI: payments, deposit-taking and management, custody, settlements and clearing;

(b) for an insurer (general, life, private health): claims processing;

(c) for an RSE licensee: investment management and fund administration; and

(d) for all APRA-regulated entities: customer enquiries and the systems and infrastructure needed to support critical operations.

37. APRA may require an APRA-regulated entity, or a class of APRA-regulated entities, to classify a business operation as a critical operation.

38. For each critical operation, an APRA-regulated entity must establish tolerance levels for:

(a) the maximum period of time the entity would tolerate a disruption to the operation;

(b) the maximum extent of data loss the entity would accept as a result of a disruption; and

(c) minimum service levels the entity would maintain while operating under alternative arrangements during a disruption.

39. APRA may require an APRA-regulated entity to review and change its tolerance levels for a critical operation. APRA may set tolerance levels for an APRA-regulated entity, or a class of APRA-regulated entities, where it identifies a heightened risk or material weakness.

Business continuity plan

40. An APRA-regulated entity's BCP must include:

(a) the register of critical operations and associated tolerance levels;

(b) triggers to identify a disruption and prompt activation of the plan, and arrangements to direct resources in the event of activation;

(c) actions it would take to maintain its critical operations within tolerance levels through disruptions;

(d) an assessment of the execution risks, required resources, preparatory measures, including key internal and external dependencies needed to support the effective implementation of the BCP actions; and

(e) a communications strategy to support execution of the plan.

41. An APRA-regulated entity must maintain the capabilities required to execute the BCP, including access to people, resources and technology. An APRA-regulated entity must monitor compliance with its tolerance levels and report any failure to meet tolerance levels, together with a remediation plan, to the Board.

42. An APRA-regulated entity must notify APRA as soon as possible, and not later than 24 hours after, if it has suffered a disruption to a critical operation outside tolerance. The notification must cover the nature of the disruption, the action being taken, the likely impact on the entity's business operations and the timeframe for returning to normal operations.

Testing and review

43. An APRA-regulated entity must have a systematic testing program for its BCP that covers all critical operations and includes an annual business continuity exercise. The program must test the effectiveness of the entity's BCP and its ability to meet tolerance levels in a range of severe but plausible scenarios.

44. The testing program must be tailored to the material risks of the APRA-regulated entity and include a range of severe but plausible scenarios, including disruptions to services provided by material service providers and scenarios where contingency arrangements are required. APRA may require the inclusion of an APRA-determined scenario in a business continuity exercise for an APRA regulated entity, or a class of APRA-regulated entities.

45. An APRA-regulated entity must update, as necessary, its BCP on an annual basis to reflect any changes in legal or organisational structure, business mix, strategy or risk profile or for shortcomings identified as a result of the review and testing of the BCP.

46. An APRA-regulated entity's internal audit function must periodically review the entity's BCP and provide assurance to the Board that the BCP sets out a credible plan for how the entity would maintain its critical operations within tolerance levels through severe disruptions and that testing procedures are adequate and have been conducted satisfactorily.

30. Business continuity is achieved through a combination of controls that reduce the likelihood and/or impact of a business disruption. This approach may include measures to minimise the immediate impact of a disruption; activate contingency arrangements; and facilitate the recovery of critical operations.

Maintain a register of critical operations, set tolerance levels

31. An entity's register of critical operations would typically include:

    a) the name of the critical operation;

    b) a description of the critical operation;

    c) tolerance levels for disruptions; and

    d) the material service provider arrangements supporting the critical operation.

32. In setting and reviewing tolerance levels, a prudent entity would consider:

    a) the impact on its customers and other stakeholders of a disruption;

    b) the financial and reputational impact on the entity from a prolonged or material disruption;

    c) the financial and reputational impact on the broader financial system, including any flow-on effects or contagion;

    d) legal or regulatory requirements, including any tolerance levels set by APRA; and

    e) recovery objectives.

33. APRA expects that entities will reassess tolerance levels as they learn lessons from actual disruptions, testing, scenario analysis and evolution in industry practices.

Table 4. Types of tolerance levels for disruptions

Tolerance type	Factors to consider in setting tolerances
Maximum period	Maximum allowable disruption (the maximum amount of time a business service can be unavailable before the impact is deemed unacceptable). Recovery time objectives (the maximum amount of time allowed for the recovery of information assets that relate to a business service).
Maximum data loss	Recovery point objective (the maximum amount of data loss that the business can tolerate in terms of time). This is typically measured by how far back the business can reconstruct data through other techniques such as re-keying and is normally used to inform the frequency of point-in-time backups.
Minimum service levels	Recovery level objective (the minimum level of service that needs to be restored to avoid impacts that are deemed unacceptable). An entity would normally establish a recovery level objective when resumption to business-as-usual operations may take a long time. An entity would normally determine the minimum level of people, information assets and other resources required to provide the business service.

Maintain a BCP, be ready to activate it

34. An entity's BCP caters to all stages of disruption to critical operations: triggers and identification; initial actions (such as alternative arrangements); further actions; assessment; and communications.

35. The use of contingency arrangements (where viable options exist) enables entities to respond quickly to a disruption when recovery plans do not operate as intended, including those of service providers and related parties.

36. An entity may maintain one or more BCPs and would be able to enact these quickly when required. It is useful to clearly link the BCP and any other management plans that deal with incidents, including disaster recovery, liquidity management and information security incident management. Alignment with crisis management governance, triggers, actions and communication plans is important.

Test the BCP

37. Testing the BCP should highlight any deficiencies, build experience in managing a crisis and strengthen the plan. Systematic testing of BCPs and associated disaster recovery plans would typically occur over a multi-year cycle, during which all critical operations would be considered (for example, over a three-year cycle).

38. Test results and the execution of any findings such as remediation would be reported to and reviewed by the Board, with associated follow-up actions formally tracked and reported. Reports on BCP tests would typically include:

    a) the scope, including the critical operations included (and excluded) and the specific tolerance levels tested;

    b) what was demonstrated by the test, including whether tolerance levels were met; and

    c) any issues raised, root causes and required remediation, including timeframes and accountabilities for actions.

39. Entities that rely on material service providers would seek to confirm that those providers also maintain robust BCP testing. Joint testing of arrangements with the service provider could be considered.

Update the BCP

40. An entity must review and update its BCP annually, and as soon as possible after a material change in the entity's structure, business or risk profile, such as after a merger or acquisition or a major external shock.

41. BCPs should be informed by results of testing, internal audit findings and lessons learned from actual business disruptions.

Audit the BCP

42. Internal audit is an important vehicle for assurance. The Board may consider seeking assurance through expert opinion or other means to complement internal audit.

43. An audit program would typically assess all aspects of business continuity capability over time. Additional assurance projects could be triggered by changes to services, processes, information assets, the business environment and stakeholder expectations.

Management of service provider arrangements

47. An APRA-regulated entity must maintain a comprehensive service provider management policy. The policy must cover how the entity will identify material service providers and manage service provider arrangements, including the management of material risks associated with the arrangements.

48. The policy must include:

(a) the entity's approach to entering into, monitoring, substituting and exiting agreements with material service providers;

(b) the entity's approach to managing the risks associated with material service providers; and

(c) the entity's approach to managing the risks associated with any fourth parties that material service providers rely on to deliver a critical operation to the APRA-regulated entity.

Material service providers

49. An APRA-regulated entity must identify and maintain a register of its material service providers and manage the material risks associated with using these providers. Material service providers are those on which the entity relies to undertake a critical operation or that expose it to material operational risk. Material arrangements are those on which the entity relies to undertake a critical operation or that expose it to material operational risk.

50. An APRA-regulated entity must, at a minimum, classify a provider of the following services as a material service provider, unless it can justify otherwise:

(a) for an ADI: credit assessment, funding and liquidity management and mortgage brokerage;

(b) for an insurer (general, life, private health): underwriting, claims management, insurance brokerage and reinsurance;

(c) for an RSE licensee: fund administration, custodial services, investment management and arrangements with promoters and financial planners; and

(d) for all APRA-regulated entities: risk management, core technology services and internal audit.

51. An APRA-regulated entity must submit its register of material service providers to APRA on an annual basis.

52. APRA may require an APRA-regulated entity, or a class of APRA-regulated entities, to classify a service provider, type of service provider or service provider arrangement as material.

Service provider agreements

53. Before entering into or materially modifying a material arrangement, an APRA-regulated entity must:

(a) undertake appropriate due diligence, including an appropriate selection process and an assessment of the ability of the service provider to provide the service on an ongoing basis; and

(b) assess the financial and non-financial risks from reliance on the service provider, including risks associated with geographic location or concentration of the service provider(s) or parties the service provider relies on in providing the service.

54. For all material arrangements, an APRA-regulated entity must maintain a formal legally binding agreement (formal agreement). The formal agreement must, at a minimum:

(a) specify the services covered by the agreement and associated service levels;

(b) set out the rights, responsibilities and expectations of each party to the agreement, including in relation to the ownership of assets, ownership and control of data, dispute resolution, audit access, liability and indemnity;

(c) include provisions to ensure the ability of the entity to meet its legal and compliance obligations;

(d) require notification by the service provider of its use of other material service providers that it materially relies upon in providing the service to the APRA-regulated entity through sub-contracting or other arrangements;

(e) require the liability for any failure on the part of any sub-contractor to be the responsibility of the service provider;

(f) include a *force majeure* provision indicating those parts of the contract that would continue in the case of a *force majeure* event; and

(g) termination provisions including, but not limited to, the right to terminate both the arrangement in its entirety or parts of the arrangement. For an RSE licensee, termination provisions must include the ability for the RSE licensee to terminate the arrangement where to continue the arrangement would be inconsistent with the RSE licensee's duty to act in the best financial interests of beneficiaries (refer to subsection 52(2)(c) of the SIS Act).

55. The formal agreement must also include provisions that:

(a) allow APRA access to documentation, data and any other information related to the provision of the service;

(b) allow APRA the right to conduct an on-site visit to the service provider; and

(c) ensure the service provider agrees not to impede APRA in fulfilling its duties as prudential regulator.

56. For each material arrangement, an APRA-regulated entity must:

(a) identify and manage risks that could affect the ability of the service provider to provide the service on an ongoing basis;

(b) identify and manage risks to the APRA-regulated entity that could result from the arrangement, such as step-in risk or contagion risk;

(c) ensure it can execute its BCP if needed; and

(d) ensure it can conduct an orderly exit from the arrangement if needed.

57. APRA may require an APRA-regulated entity to review and make changes to a service provider arrangement where it identifies heightened prudential concerns.

Monitoring, notifications and review

58. An APRA-regulated entity must monitor and ensure that senior management receive reporting on material arrangements commensurate with the nature and usage of the service. This monitoring must include a regular assessment of:

(a) performance under the service agreement with reference to agreed service levels;

(b) the effectiveness of controls to manage the risks associated with the use of the service provider; and

(c) compliance of both parties with the service provider agreement.

59. An APRA-regulated entity must notify APRA:

(a) as soon as possible and not more than 20 business days after entering into or materially changing an agreement for the provision of a service on which the entity relies to undertake a critical operation; and

(b) prior to entering into any material offshoring arrangement, or when there is a significant change proposed to the arrangement, including in circumstances where data or personnel relevant to the service being provided will be located offshore.

60. An APRA-regulated entity's internal audit function must review any proposed material arrangement involving the outsourcing of a critical operation. The internal audit function must regularly report to the Board or Board Audit Committee on compliance of such arrangements with the entity's service provider management policy.

Maintain a service provider management policy

44. Where an entity uses a service provider, the entity still owns and is responsible for managing its risk. The service provider management policy must set out how this is to be done.

45. In addition to those matters set out in CPS 230, a service provider management policy would usually include:

    a) roles and responsibilities of Accountable persons or equivalent;

    b) processes for the selection of and due diligence on service providers;

    c) methodology for the assessment of the materiality of service providers;

    d) on-boarding and exiting procedures;

e) BCPs and alternative arrangement considerations (including where the service provider is unable to provide the service for an extended period of time);

f) issues management and escalation procedures;

g) processes for vetting key personnel of service providers; and

h) oversight processes and practices to monitor the service providers, service level agreements and risks.

Maintain a register of material service providers

46. Material service providers are those on which the entity relies to undertake a critical operation or that expose it to material operational risk. Paragraph 50 of CPS 230 prescribes a minimum list of material service providers, which provides a starting point for entities developing their register of material service providers.

47. For the purposes of the register, CPS 230 does not intend to capture arm's length transactions or intermediation unless they meet criteria under paragraph 49 of CPS 230. For example, the purchase of reinsurance or the intermediation of an insurance policy by a broker would not mean that the provider of the service would automatically be deemed a material service provider and need to be captured in the register. Rather, CPS 230 is intended to capture those arrangements where an entity relies on a service provider to undertake a critical operation, or the arrangement introduces material operational risk to the entity.

48. In developing its material service provider register, a prudent entity would:

    a) include a list of the entity's material arrangements, and identify the responsible person for each arrangement within the entity;

    b) identify which critical operation(s) the material arrangement supports, and/or which material risk the arrangement connects to in the entity's risk profile; and

    c) where the material arrangement is relied on to deliver a critical operation, take reasonable steps to list fourth parties involved in delivery of the critical operation.

49. APRA expects that where an entity decides not to classify a service provider prescribed by APRA as material, the reasons would be documented, approved by an Accountable person and reviewed on at least an annual basis. It is not necessary to provide the documented reasoning to APRA, unless APRA specifically requests an entity to provide this information.

Manage risks associated with material service providers

50. Entities should proactively manage the key risks associated with material arrangements. Entities' BCPs would account for these key risks and have contingencies to limit disruption of critical operations. Entities would also look to satisfy themselves that their material service providers' risk management practices and BCPs are similarly robust.

51. A prudent entity would manage the operational risk associated with cohorts of service providers, where the aggregate impact is material, but each individual provider is not. This does not mean that each service provider in the cohort needs to be identified as a material service provider, but rather that the entity has additional processes and controls in place to satisfy itself that the operational risks of such cohorts are being monitored and managed.

Maintain agreements for material arrangements

52. CPS 230 requires entities to maintain formal agreements for material arrangements with material service providers. Not all arrangements with a material service provider will be material to support delivery of the critical operation or expose the entity to material operational risk.

Monitor performance

53. An entity would normally conduct periodic reviews of material arrangements with a service provider. This could include assessment of operational issues (including information security incidents and service disruptions); control effectiveness; information security capabilities and business continuity capabilities; strategic changes; and comparisons to other offerings in the market.

Assess risk when engaging a new material service provider

54. When selecting and assessing a prospective provider of material arrangements, an entity would typically consider the following against its risk appetite:

    a) business services and capabilities which must be retained in-house;

    b) country or region risk;

    c) supplier risk;

    d) concentration risk; and

    e) reputational risk.

55. A prudent entity would assess the risks of engaging a service provider in another jurisdiction to determine if it is within appetite. This would include consideration of:

    a) the ability to continue operations and meet core obligations following a loss of service;

    b) maintenance of information security;

    c) the ability to own and manage controls on its behalf;

    d) compliance with legislative and prudential requirements; and

    e) impediments, legal and technical, to APRA being able to fulfil its duties, including timely access to information in a usable form.

56. Where an entity proposes to outsource a critical operation, or part thereof, currently performed in-house, the proposed outsourcing is to be reviewed by internal audit before any final decision is made. A prudent entity would ensure its internal audit function has sufficient capability and capacity to undertake the required review.